UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/645,953 | 08/22/2003 | Vipin Samar | OR03-10201 | 8253 |

51067 7590 11/12/2008

PVF -- ORACLE INTERNATIONAL CORPORATION
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

| EXAMINER |
|---|
| LEE, WILSON |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2163 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/12/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/645,953 | SAMAR, VIPIN | |
| | Examiner | Art Unit | |
| | Wilson Lee | 2163 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,4-6,8-10,12-14 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-6,8-10,12-14 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**Continued Examination Under 37 CFR. 1.114**

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued under 37 CFR 1.114, and fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10-31-08 has been entered.

**Response to Arguments**

Applicant's arguments filed on 10/31/08 have been fully considered but they are not persuasive.

**Argument #1**

Applicant argues that neither De Vries nor Trostle discloses a system wherein the hash of the item of private information is created by the database in a manner that is transparent to an application which manipulates the private information because, as alleged by applicant, in De Vries, the **hash is calculated on a trusted computer**, and the **hash is then sent to the database** on an un-trusted network.

Examiner respectfully disagrees.

First, the database as claimed (Claim 1, lines 1-2) is the **database that creates the hash of the private information and is protected**.

Analogously, De Vries teaches a database that **creates the hash of the private information (e.g. confidential information) and is protected from the un-trusted network or computers is the database of the trusted computer**. The following teachings in De Vries support Examiner's position.

In Col. 2, lines 7-18, De Vries teaches "…the form of a set of query, answer pairs, where the query hash is represented as a hash result that is a one way hashing function of a set of query input values. This set of query, answers pairs is distributed to other computers…"

As shown above, the hash result has been created **before** as being distributed to other computers.

Further, applicant admits that "…because De Vries teaches that the private information **is hashed prior to delivering** it to the database", on page 7, lines 12-13.

Therefore, the hash result must be created in the database of the trusted computer **prior to** or **before** as being distributed to other computers, or other databases of un-trusted network.

The purpose of De Vries invention is to put the information into one-way hash function, then distribute them in an intelligible form to other computers so that other computers cannot access the confidential information.

For examples,

In Col. 1, lines 59-67 and Col. 2, lines 1-6, De Vries teaches "...confidential information **without making the confidential information available to un-trusted** information processing servers…"

In Col. 2, lines 19-22, De Vries teaches "This form of black box encapsulation ... **protects the confidential information from** discovery on the computers..."

Second, applicant mistakenly equates the database on the un-trusted network of De Vries to the protected database as claimed. The database on the un-trusted network of De Vries is **not** the database that creates the hash result and is protected by the method. In fact, the database on the trusted computer of De Vries is the database that creates hash result and is protected by the method.

Regarding "…in a manner that is transparent to an application which manipulates the private information."

De Vries does teach the information in a manner that is transparent (e.g. invisible, not accessible, without revealing, without making confidential information available, in a manner from which the confidential information cannot be explicitly derived) to an application (at the other computers or untrusted network) which manipulates the private information.

The following recitations in De Vries support Examiner's position.

In Col. 1, lines 59-60, De Vries teaches "… distribute processing based on confidential information <u>without making the confidential information available to untrusted</u> information processing servers..."

In Col. 2, lines 1-2, De Vries teaches "information in a manner from which confidential information <u>cannot be explicitly derived</u> …"

In Col. 2, lines 11-15, De Vries teaches "...can then effectively query the confidential information without having access to or directly processing the raw confidential information…"

In Col. 2, lines 29-32, De Vries teaches "the set of query input values is not visible from the query".

In Col. 7, lines 9-16, "…the logic … remains at the trusted computer and inaccessible to the query computer."

Further, De Vries teaches "query comprising a set of the query input values is hashed…The hash result of the query is used as look-up into the set of the query...", in Col. 2, lines 7-18. De Vries' above teaching perfectly matches the definition of "transparent to application" defined in the instant specification on page 6, lines 23 to page 7, line 2.

**Argument #2**

Applicant argues that De Vries fails to disclose "creating an index based on the hash."

Examiner respectfully disagrees.

De Vries does teach creating an index (look up index) based on the hash.

The following recitations in De Vries support Examiner's position.

De Vries, Abstract, lines 8-10, "The query is performed on such other computers by hashing the query terms, using the resulting query hash as a look up index to the associated answer in the querying data structure"

De Vries. Col. 11, lines 26-34, "calculating an answer look up index as the one way hashing function of the query's input term values; looking up a query hash value and answer value pair in the data set that is indexed by the answer look-up index".

**Claim Rejections – 35 U.S.C. 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-6, 8, 9, 12-14, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Vries (6,928,428) in view of Hild et al. (6,763,440).

Regarding Claim 1, De Vries discloses a method for protecting an item of private information in a database, wherein the method comprises:

receiving (input data set. When the data is inputted to the system, it means the system receives the data) the item of private information (Col. 5, lines 3-24), wherein the item of private information is used as a key for retrieving data from the database (Col. 2, lines 14-18);

creating a hash of the item of private information at a database (Col. 2, lines 1-18), wherein creating the hash further comprises checking a column attribute for a column, which stores the item of private information, in the database to determine that "privacy" is enabled for the column, and only upon privacy being enabled for the column ("…input data set 310...as a flat database table in row/colum format (i.e., where columns represent fields of the input data, such as contact name...", Col. 5, lines 3-24)[1], creating the hash, wherein the hash of the item of private information is created (Col. 2, lines 7-18 and see explanation in the arguments above) by the database in a manner that is transparent (Col. 1, lines 59-60; Col. 2, lines 1-2, line 11-15, lines 29-32, lines 7-18 and Col. 7, lines 9-16 and see explanation in the arguments above) to an application (at the other computers or untrusted network) which manipulate the private information (querying the information or having information being distributed to the other computer); and wherein the hash is a one-way hash ("…produces a hash value that is one-way hashing function of at least some of the input data set fields…", Col. 5, lines 24-35); and

storing the hash of the item of private information in the database (Col. 5, lines 3-35), wherein the hash of the item of private information (refer to "confidential information" such as contact name, calendar date/time, location, etc) is a unique lookup key within the database ("the query data structure 220 takes the form of a set of query hash and answer pairs, which is constructed from an input data set 310 that represents the user context data 210...", Col. 5, lines 3-24 and "…using the resulting query hash as a look up index to the associated answer in the querying data structure, and acting on the answer…", Abstract),

and wherein the item of private information does not exist in the database in plain-text form ("without making the confidential information available to un-trusted information processing servers in an intelligible form (i.e. plain text)", Col. 1, lines 59-63);

creating an index based on the hash (Abstract, lines 8-10 and Col. 11, lines 26-34 and see explanation in the arguments above); and

As discussed above, De Vries discloses rejecting the item of private information (Col. 1, lines 59-63 and Col. 7, lines 1-16) being accessible to other computers or untrusted network. Although De Vries does not literally disclose discarding the item of private information, however, Hild (6,763,460) teaches that it is advantageous that the encrypted confidential information data is removed (Col. 3, lines 19-51). Therefore, it would have been obvious to one of ordinary skill in the art to have removed or discarded the confidential information in De Vries in order to attain advantageous benefit of increasing transmission security, and/or minimizing external fraudulent influence as taught by Hild.

Regarding Claim 4, De Vries discloses that processing a query containing the private information involves:

receiving (input data set. When the data is inputted to the system, it means the system receives the data) the item of private information (Col. 5, lines 3-24);

creating a hash of the item of private information ("…query hash and answer pairs…are produced…", "The resulting query hash value", Col. 5, lines 3-35; Col. 2, lines 1-18); and

querying the database using the hash of the item of private information ("querying of confidential information", "hashing the query", using the resulting query hash", "to the query hashes in the query data structure by reverse hash", Abstract; Fig. 3; Col. 2, lines 7-18; ).

Regarding Claim 5, De Vries discloses that the item of private information can include a person's name ("contact name", Col. 5, lines 3-13).

---

[1] De Vries teaches that the input data set as the item of private information stored in the column of the table.

Regarding Claim 6, De Vries discloses that multiple items ("input data, such as contact name, calendar date/time, location, etc.", Col. 5, lines 3-13) of private information can be combined prior to creating the hash (Examiner's note: the input data is prior to the hash. See Col. 5, lines 24-35).

Regarding Claim 8, De Vries discloses that the database is a Lightweight Directory Access Protocol (LDAP) database ("…devices 120-123 and information services can use standard data networking protcols…LDAP", Col. 3, lines 29-33).

Regarding Claim 9, as discussed in details in the preceding rejection of claim 1, De Vries/Hild meets the limitation of claim 9.

Regarding Claim 12, as discussed in details in the preceding rejection of claim 4, De Vries/Hild meets the limitation of claim 12.

Regarding Claim 13, as discussed in details in the preceding rejection of claim 5, De Vries/Hild meets the limitation of claim 13.

Regarding Claim 14, as discussed in details in the preceding rejection of claim 6, De Vries/Hild meets the limitation of claim 14.

Regarding Claim 16, as discussed in details in the preceding rejection of claim 8, De Vries/Hild meets the limitation of claim 16.

Claims 2 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Vries (6,928,428) in view of Hild et al. (6,763,440), further in view of the term dictionary in Javvin (This reference has been made in record. Please see previous Form 892 dated 02/05/2008).

Regarding Claims 2 and 10, as discussed above, De Vries/Hild essentially discloses the claimed invention but does not explicitly disclose creating the hash can include creating either Secure Hash Algorithm-1 (SHA-1) or Message-Digest algorithm 5 (MD5) hash. However, Javvin dictionary teaches that Message-Digest algorithm 5 (MD5) (designed in 1991) is a popular algorithm in security application and to check the integrity of files. And Javvin also discloses that SHA-1 is recommended by cryptographers to overcome some flaws in MD5. It would have been obvious to one of ordinary skill in the art at the time the invention has been made to use either MD5 or SHA-1 in De Vries/Hild in order to

provide additional security purpose since both MD5 and SHA-1 are widely used and known to a skilled in the art.

Claims 2 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Vries (6,928,428) in view of Hild et al. (6,763,440), further in view of Tuvey et al. (2002/0019849).

Regarding Claims 2 and 10, as discussed above, De Vries/Hild essentially discloses the claimed invention but does not explicitly disclose creating the hash can include creating either Secure Hash Algorithm-1 (SHA-1) or Message-Digest algorithm 5 (MD5) hash. However, Tuvey teaches that Message Digest algorithm 5 (MD5) is one way hash algorithm being used for resisting collision (paragraph 0053). It would have been obvious to one of ordinary skill in the art to have used MD5 such standard one way hash algorithm in De Vries/Hild in order to resist collision as taught by Tuvey.

**Conclusion**

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Pitsos (US 2006/0129847) teaches that it is advantageous for large amounts of data that has been distributed and encrypted using one specific key pair when the private key is removed or deleted (paragraph 0091).

**Correspondence**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Wilson Lee whose telephone number is (571) 272-1824. Papers related to the application may be submitted by facsimile transmission. Any transmission not to be considered an official response must be clearly marked "DRAFT". The official fax number is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

11-7-08

/Wilson Lee/
Primary Examiner, Art Unit 2163